Strategy Research Project

Cyber Warfare: New Character with Strategic Results

by

Colonel James B. Dermer
United States Air Force

United States Army War College
Class of 2013

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
xx-03-2013	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Cyber Warfare: New Character with Strategic Results

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Colonel James B. Dermer
United States Air Force

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Colonel Joseph C. Dill
Department of Command, Leadership, and Management

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 6995

14. ABSTRACT

The advent of cyber warfare sparked a debate amongst theorists as to whether timeless Clausewitzian principles remain true in the 21st century. Violence, uncertainty, and rationality still accurately depict the nature of cyber warfare, however, its many defining attributes and means by which this style of warfare is conducted has definitively changed the character of war. Although cyber warfare is contested in the cyber domain, it often creates kinetic effects of strategic value. This statement is especially true as societies become more and more dependent on the integration of cyberspace in governance, economies, and critical services. While the strategic effectiveness of cyber warfare is untested, computer network attack is capable of attacking enemy centers of gravity through critical vulnerabilities. In conflicts with limited strategic endstates, cyber warfare has the potential to bend the will of an enemy and create decisive strategic effects within the confines of the cyber domain.

15. SUBJECT TERMS
Nature of War; Character of War; Strategic Decisiveness

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(Include area code)*
UU	UU	UU	UU	34	

USAWC STRATEGY RESEARCH PROJECT

Cyber Warfare: New Character with Strategic Results

by

Colonel James B. Dermer
United States Air Force

Colonel Joseph C. Dill
Department of Command, Leadership, and Management
Project Adviser

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title:	Cyber Warfare: New Character with Strategic Results
Report Date:	March 2013
Page Count:	34
Word Count:	6995
Key Terms:	Nature of War; Character of War; Strategic Decisiveness
Classification:	Unclassified

The advent of cyber warfare sparked a debate amongst theorists as to whether timeless Clausewitzian principles remain true in the 21st century. Violence, uncertainty, and rationality still accurately depict the nature of cyber warfare, however, its many defining attributes and means by which this style of warfare is conducted has definitively changed the character of war. Although cyber warfare is contested in the cyber domain, it often creates kinetic effects of strategic value. This statement is especially true as societies become more and more dependent on the integration of cyberspace in governance, economies, and critical services. While the strategic effectiveness of cyber warfare is untested, computer network attack is capable of attacking enemy centers of gravity through critical vulnerabilities. In conflicts with limited strategic endstates, cyber warfare has the potential to bend the will of an enemy and create decisive strategic effects within the confines of the cyber domain.

Cyber Warfare: New Character with Strategic Results

War is a complex act based upon dynamic political, socio-cultural, economic and technological drivers. Over the course of centuries, the means to conduct war evolved from foot soldiers and naval ships to include cutting-edge technologies such as stealth aircraft and unmanned aircraft systems. This evolutionary warfare trend continued in the latter part of the 20th century with the emergence of new technologies derived from the advent of the Internet and networked information systems. Today, militaries leverage a manmade cyberspace domain to increase the speed, agility, and lethality of war.

Along with the militarization of cyberspace was a parallel advance in the civilian sector. Developed societies quickly became dependent upon networked technology to control critical infrastructure (i.e. the national power grid, air traffic control, railroads, and marine navigation), world financial markets, news media distribution, communications infrastructure, global supply chains, and vital human services. Consequently, the maintenance of a secure and reliable networked cyber infrastructure became critical to the developed world's security.

With the expanded reliance on networked systems came a resultant increase in vulnerabilities. Not only are these systems at risk to criminal and espionage exploitation, but also they are also vulnerable as military targets in both the physical and cyberspace domain. States now possess the ability to attack an adversary's networked technologies, including critical infrastructure, directly through the cyberspace domain without regard to distance, proximity of forces, or supply constraints.

Because of its strategic economic and military value, the cyberspace domain is exploited daily. In fact, the U.S. Department of Defense acknowledged its networks are scanned or attacked millions of times each day.[1] Threats originate from multiple states

and non-state actors whose motivations span from criminal and espionage to overt military action.[2] Examples of these activities range from: an innocuous computer virus with limited aims; a distributed denial of service attacks meant to overwhelm servers; to malware designed to disrupt or destroy key infrastructure. State sponsored cyber espionage is particular devastating and costly to the industrial base. In 2008, industry estimates exceeded a loss of $1 trillion in trade secrets, intellectual property and corporate bargaining strategies.[3] Although the U.S. media characterizes many of these acts as part of a greater cyber war, most are considered acts of cyber crime or espionage. Making delineation between cyber crime, cyber espionage, and other malicious cyber acts is not clear-cut and often stems from motivation or intent.[4]

This difference in intent was evident in 2008 when Russia executed a distributed denial of service attack on numerous government of Georgia websites as a prelude to a five-day conventional conflict. While the effectiveness of this cyber attack is still debated, it proved disruptive to Georgia's command and control systems and set a precedent for the future integration of cyber and conventional force attacks.

Aside from the additive contribution to convention warfare, new theories speculate the effects of an independent application of cyber warfare. Pertinent questions include whether cyber warfare capability can mature to a level where it produces strategic results independent of other domains of warfare? If it is possible to independently achieve strategic effects, is the unrestricted use of cyber warfare legal or must the application of this new form of warfare conform to any established international norms of behavior? Finally, if these effects are plausible, has the use of the cyber domain fundamentally changed the character of war?

Problem Statement

The application of cyber warfare is still in its infancy. Everyday state and non-state actors are applying a range of cyber force for varying purposes. Frequently the motivations are criminal, often they are exploitive (i.e. cyber espionage), and increasingly they have been provocative (i.e. threatening critical infrastructure).[5] While the activities of all actors operating in this domain are pertinent, this paper focuses on the effects created by states.

As with any type of warfare, strategic results are the ultimate effectiveness test. Accordingly, there is much debate regarding the decisiveness of cyber warfare. Since no states have attempted to break an enemy's will through the exclusive use of cyber operations, this paper extrapolates its plausibility through an examination of current capabilities. Furthermore, it is relevant to analyze whether cyber warfare will transform the character of war or serve as just another weapon in a conventional force arsenal.

While the intent of this paper is not to advocate a single domain approach to warfare, there are circumstances which may drive this eventuality. In situations where a conflict averse political system is confronted with a complex problem, options which enable a government to coerce or bend the will of another state without the large footprint and cost of conventional forces is worthy of further study. Therefore, the purpose of this research is to describe how cyber warfare changes the character of war and how it is capable of producing decisive strategic effects in a war with limited objectives.

Review of Literature

Definitions and Terminology

Because cyberspace is a relatively new domain, there is an absence or frequent inconsistency in much of the terminology associated with this form of warfare. The following section draws from many accepted journal articles and books to establish a baseline for this paper.

General Keith Alexander, Commander of United States Cyber Command, defines cyber warfare as the use of cyberspace "to attack personnel, facilities, or equipment with the intent of degrading, neutralizing or destroying enemy combat capability, while protecting our own."[6] General Alexander's description of cyber warfare does not expressly limit the means exclusively to computer network operations. In his article, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," Adam Liff further refines General Alexander's definition as "including only computer network attacks (CNA) with direct political and/or military objectives – namely, attacks with coercive intent and/or as a means to some strategic and/or brute force end – and computer network defense (CND)."[7] Thus cyber warfare is distinguished from cyber criminal acts based upon its coercive nature to attain a strategic end, whereas cyber crime is a means to a profit.

Another significant term requiring a specific definition is cyber war. While cyber warfare is a means to an end, cyber war is the actual engagement of two states attacking each other's networks and cyber-supported systems solely through the cyberspace domain.[8] This definition is a key departure from other forms of war because it restricts its use to a single domain despite the current trend to integrate CNA within multi-domain operations. While a purest interpretation of cyber war is restricted to a

specific domain, its effects can be manifested to the physical world. For example, in 2010 a CNA named Stuxnet altered the code of the Supervisory Control and Data Acquisition systems used to operate Iranian centrifuges. The malware caused variations to the speed and vibration levels to "nearly 1,000 of the 5,000 centrifuges Iran had spinning at the time to purify uranium."[9] This attack successfully delayed the Iranian effort to enrich uranium.

The two key components of cyber warfare are CNA and CND. Conceptually, CNA effects "range from disrupting the adversary's electronic systems and what operations they enable (communications, guidance systems, radar capabilities, etc.) to actual kinetic damage accomplished by using cyber tools to cause an adversaries system to malfunction or self-destruct."[10] The second component of cyber warfare seeks to eliminate or minimize the risk of the first. The role of CND is to defend networks from attack either through passive or active measures. Passive defenses are traditional measures such as virus detection and training of users on information assurance practices. Active defense uses "sensors, software, and signatures derived from intelligence to detect and stop any malicious code before it causes any damage."[11] While both CNA and CND are crucial facets of cyber war, this paper concentrates exclusively on CNA.

An additional term in the international cyber lexicon requiring clarification is "armed attack." Similar to the physical world, there is no commonly agreed upon definition for this phrase or one which easily transitions to the cyberspace domain. In the absence of an analogous definition, it is difficult to extend or invoke treaty articles in response to an "armed attack" in the cyber domain. In the physical world, an "armed

attack" can be equated to an attack upon a state, its military forces, its persons or property. The U.S. military's Standing Rules of Engagement define a hostile act as "force used directly to preclude or impede the mission and/or duties of U.S. forces, including the recovery of U.S. personnel or vital U.S. government property."[12] Applying these standards to cyberspace is contentious in the international community since millions of cyber attacks transpire daily, for which many conform to this definition. Yet, by purposefully failing to define an "armed attack" with regard to cyberspace, individual states or collective bodies do not lose credibility for failing to respond to a cyber attack.

The final term requiring an explicit definition is strategic effect. Noted strategist Colin Gray, author of *The Strategy Bridge: Theory for Practice*, defines strategic effect as "the consequences of behaviour [sic] upon an enemy. The effect can be material, psychological or both. Control is sought via restricting an enemy's ability to resist and also, perhaps, his will do so."[13] In other words, "strategic effects should neutralize the adversary's centers of gravity (COGs)."[14] These definitions are particularly apropos because cyber warfare's effects are frequently material and psychological. CNA can elicit not only kinetic consequences for an enemy, but can manifest equally damaging psychological consequences and feelings of helplessness upon their populous. The cumulative psychological and kinetic impacts directly affect the enemy's will and desire to resist.

Cyber Warfare Meets Clausewitz

Carl von Clausewitz defined war as "an act of force to compel our enemy to do our will."[15] He added that this act of force is for a political purpose in his seminal axiom that "war is simply a continuation of political intercourse, with the addition of other means."[16] This assertion is as relevant today as when originally conceived in the early

1800s. Whether one is describing a war between states, civil war insurgencies, or acts of terrorism, the common denominator is its political motivation as well as its objective nature. Clausewitz best describes this enduring nature of war as violent, uncertain, and rational.[17]

For thousands of years wars have embodied these objective traits. States battled violently on the land and sea to secure their political objectives such as the seizure of territory or regime change. And while the battlefield landscape changed over the course of time, the objective nature of the war remained constant—violent, uncertain, and rational. Physical force was the ultimate arbiter and means to bend the will of another. "Force—that is, physical force, for moral force has no existence save as expressed in the state and the law—is thus the means of war; to impose our will on the enemy is its object. To secure that object we must render the enemy powerless; and that in theory, is the true aim of warfare."[18]

While Clausewitz understood the utility of physical force, he also recognized that it was not always necessary for an enemy to be physically destroyed. In fact, conflicts are often resolved short of enemy being powerless. Clausewitz wrote:

> But the aim of disarming the enemy. . . is not in fact always encountered in reality and need not be achieved as a condition of peace. . . . Many treaties have been concluded before one of the antagonists could be called powerless—even before the balance of power had been seriously altered.[19]

Creating doubt and insecurity through the perception of overwhelming strength increases the likelihood of an adversary suing for peace prior to destruction.[20] This concept is particularly relevant to the strategic decisiveness of cyber warfare as it does not render an adversary powerless, but will create the doubt and insecurity needed to break their will.

Clausewitz suggests that the violent use of physical force is a means of imposing one's will on an adversary, but political policy determines how it is employed and to what end. As stated previously, a rational policy is central to the objective nature of war, yet it also shapes its subjective nature or war's character.[21] While Clausewitzian scholars profess the objective nature of war is enduring, its character or "means by which war has to be fought," is transient and will vary widely based upon many factors to include socio-cultural and technological shifts.[22] In his book, *Another Bloody Century: Future Warfare*, Colin Gray states that mankind will always experience war, that war and warfare "has an enduring, unchanging nature, but highly variable character."[23]

In the late 20th and early 21st centuries, the technology revolution greatly influenced the character of war as witnessed by the introduction of the air, space, and cyber domains. While operations within the cyberspace domain are still relatively immature, its integrated use has dramatically influenced the manner in which wars are fought. Cyber technologies have enhanced command and control, battlefield communication, targeting solutions, and logistical capability. Furthermore, an integrated use of cyber technology provides synergistic effects for systems operating in every other domain.

In the cyber era, technology permits attacks at light speed and negates any barriers imposed by distance. Forces can be equipped for as little as the price of a laptop computer. "The technologies of cyber warfare, including many of those for cyber security are accessible, economically, to all. . . . This means that a state, or even a group, can equip itself at affordable cost with the technical means, and human skills, to hurt the mighty."[24] As states continue to expand their reliance on cyber-based

technologies, they simultaneously increase their vulnerability and the effectiveness of a cyber attack. In fact, the application of cyber warfare offers states the capability to contest wars exclusively within cyberspace, yet manifest decisive physical effects.

While many technological advances are often fleeting and do not alter war's character, the use of CNA is a major transformation in warfare as forces will not need to confront one another on the battlefield. Instead, the cyber domain has replaced national boundaries with firewalls, air-gapped networks, and redundant systems. Ultimately, cyber warfare has invariably altered the means of fighting and creating decisive effects and has correspondingly changed the character of war.

While harnessing the cyber domain influences the "means by which war has to be fought," can an argument be made that cyber warfare's fundamental nature also evolved?[25] As stated previously, Clausewitz found all wars to be violent, uncertain, and rational regardless of their character. Despite the radical shift in this warfare's outward appearance, there are many parallels to Clausewitz's nature of war. With regard to violence, CNA operators can exploit vulnerabilities in a wide-range of targets and create kinetic effects. For example, in 1982 the Central Intelligence Agency designed and implanted a malicious code into the control systems of Russia's trans-Siberian gas pipeline. The malware created problems with pump speeds and valve settings, which ultimately increased pressures within the pipeline to cause one of the largest non-nuclear explosions in history.[26] CNA can have equally devastating effects upon transportation infrastructure. For instance, an attack upon networks used to control rail operations could cause train derailments or collisions without any abnormal indications within control centers. While single instances of rail disruption does not equate to the

violence Clausewitz envisioned, a concentrated attack against an entire transportation network will can produce even more damaging and wide-spread effects than an isolated battle.

The use of networked technologies and information systems has steadily improved the situational awareness of military commanders, but has failed to eliminate war's uncertainty due to the forces of fog and friction. Knowledge can never be perfect, nor can cyber warfare bring certainty to moral forces or human interaction.[27] Taken together, these descriptions of cyber war are consistent with Clausewitz's essential attributes of the nature of war— rational, violent, and uncertain. This logic is supported by Gray's analysis:

> Since war will continue to be characterized [sic] by violence; human involvement; uncertainty; strategic needs; and interaction with an intelligent enemy; friction and chance will invariably continue to operate as well. It can therefore be concluded that the information age has not de-legitimised [sic] the Clausewitzian climate and nature of war. Nevertheless, the information age has introduced some significant changes to the character of war.[28]

Strategic Decisiveness

Clausewitz contended the destruction of an enemy's fighting forces and occupation of their territory are necessary conditions for victory.[29] Despite attaining these conditions, Clausewitz theorized victory could not be assured without breaking the enemy's will: "in other words, so long as the enemy government and its allies have not been driven to ask for peace, or the population made to submit."[30] Following this logic, early airpower advocates theorized the premise of bypassing enemy forces and directly attacking centers of gravity to achieve strategic effects and break the enemy's will. History has yet to provide a definitive example of this theory, however, many parallels can be drawn between airpower and cyber warfare theories. Most important is the

analogous relationship that the air or cyber domain can break the will of the people without control of a state's territory or destruction of its armed forces.

In a total war environment, Gray asserts that "war is about control of the land." However, in a limited war context, with limited goals, territorial occupation may have little bearing on the conflict outcome if an actor's ends do not include attainment or restoration of land.[31] Cyber warfare can be utilized just to "hurt" an adversary and compel them to take a desired course of action versus devastating a country with conventional forces and creating additional hostility. At its very nature cyber warfare can be both coercive and destructive. "At the strategic level, cyber attacks could be used as a coercive counter-value weapon to wreak havoc on networks in major financial centers or to disable or destroy critical physical infrastructure."[32] The ability to attack these strategic centers through CNA hinges on the policy a nation adopts, its ingenuity to find and attack vulnerabilities, and the fortitude to accept the consequences of its actions. States that foster cyber warfare capability can potentially reduce their conventional force presence in favor of a capability which is more politically palatable and can decisively "hurt" the enemy when needed.

The Law of War

Governments purposefully restrict military capability to align it with established policy. While a nation may possess the capability to decisively win a war with overwhelming military force, it often places restrictions on its use in order to conform to the laws of war which were primarily devised to reduce unnecessary suffering and destruction. Many states have adopted what is known as the Law of Armed Conflict (LOAC) to establish rules of conflict based upon customary international law and treaties, foremost being the Geneva Conventions of 1949.[33]

As stated above, possessing a capability does not guarantee its eventual use in a conflict. Once engaged in a conflict, states that have adopted LOAC must adhere to the principles of military necessity, distinction, and proportionality. In essence these principles limit engagement of combat forces to military objectives with only the degree of force needed to accomplish the legitimate military objective.[34] Furthermore, militaries must distinguish between combatants and noncombatants prior to applying force. Given these limitations, can cyber warfare attacks remain within the realm of military necessity, distinction, and proportionality and still be decisive?

While CNA against critical infrastructure has the potential to elicit strategic effects, the question of military necessity and distinction must be considered prior to its targeting. Further obfuscating this issue is whether or not the use of cyber assets can be classified as an "armed attack." As of 2010, there was no legal entity known as cyber war. "The only issue that has been defined by international agreement is a nation's right to self-defense when attacked, and that applies only to the traditional manner of attack, i.e., 'armed' attack."[35] While international law does not directly address cyber warfare, it is clear most states recognize the effects of CNA and may purposefully avoid treaties or conventions which restrict operational capability.

When addressing the use of force and acts of war, the international community often looks to the United Nations (U.N.) for precedent. U.N. Articles 2(4), 39, and 51 give legitimacy to a state's defense following the use of force or an attack by another state. Article 2(4) states, "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state."[36] Article 39 states, "Security Council shall determine the existence of any threat

to the peace, breach of the peace, or act of aggression."[37] Finally Article 51 upholds the right to self-defense against an armed attack and provides legitimacy for a nation defending itself.[38]

While the articles outlined above provide a legitimate basis to respond to an attack or imminent attack, it does not necessarily extend to a cyber warfare attack. The germane words in these articles regarding cyber warfare are the "use of force" and "armed attack." Traditionally, the use of force has been equated to military force (i.e. bullets and bombs creating kinetic effects). While this interpretation sufficed for past conflicts, it fails to settle the debate on the application of cyber force. Further complicating the issue is the absence of what defines an "armed attack" in the U.N. Charter.[39] Scholars developed multiple models to assist with an analogous comparison of "armed attack." The first requires an attack to achieve the same damage as a kinetic attack.[40] Another test is more liberal and is based on the effects of a cyber attack.[41] For instance, manipulating data "across a state's banking and financial institutions to seriously disrupt commerce in the state is an armed attack."[42] Other interpretations require a higher threshold for invoking Article 51. "[O]nly large scale cyber attacks on critical infrastructures that result in significant damage or human losses comparable to those of an armed attack with conventional weapons would entitle the victim state to invoke self-defense under Article 51 of the U.N. Charter."[43]

Ultimately, the lack of specificity in international law forces states to determine what constitutes an armed attack in the cyber domain. Furthermore, not all states will apply similar interpretations of LOAC principles. Some states may explore the full capability of CNA without regard to military necessity, distinction, or proportionality in

order to achieve strategic effects, while others will constrain themselves by these guiding principles. In the end, an international dialogue addressing this ambiguity would promote greater transparency and stability among state actors operating within this immature, but critical domain.[44]

Analysis

War in the 21st century has many contrasts and similarities to those fought since the Treaty of Westphalia was signed in the mid-17th century. The motives for many wars following the treaty were often regime change and expansion of territory. In the late 20th century, interstate conflicts became more limited in nature. While wars remained politically motivated, policy limitations restricted the scope and conduct of war. To date, state-sponsored cyber attacks have not triggered a call to total war by a victimized state. Cyber warfare, as with other domains, is constrained by politics which limit the full realization of its capability. This restraint keeps lower spectrum cyber attacks from escalating into widespread conflict.

Despite new policies that favor more limited means and goals, states continue to build their conventional force arsenals. This arms buildup enables wealthier states to improve their security in nearly all domains. To adjust for the disparity in capabilities, less developed states and non-state actors turn to unconventional forms of warfare and harness asymmetric capabilities to confront nations or collective groups with superior means.

In the 21st century, operations in the cyber domain provide all actors a type of force-leveling which was previously reserved for the wealthy. Cyber warfare offers low entry barriers, the capability to act without regard to boundaries, reduced risk to human life, clandestine maneuver, deniability, amplified effectiveness of the few, and blurred

lines between combatant and non-combatants.[45] Even nations with large economies such as China leverage the asymmetric benefits of cyber warfare to narrow a conventional military capabilities gap between the United States and other near-peer competitors.[46]

The current and potential capability of cyber warfare continues to entice an increasing number of states to invest in CNA, CND and cyber exploitation. For instance, the United Kingdom budgeted £2.1 billion [$3.3 billion U.S.] toward its Single Intelligence account for 2011-2012 not including a classified budget for offensive cyber warfare capability.[47] Similarly, the U.S. military cyber estimates for 2012 exceeded $2.3 billion excluding additional classified funds for offensive capability.[48] While these investments fall far short of conventional force funding, it does demonstrate the value and utility of cyber warfare's contribution to their respective national defense.

Furthermore, President Barrack Obama's 2012 National Security Strategy outlines the strategic importance of a secure cyberspace.

> Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation. . . . The threats we face range from individual hackers to organized criminal groups, from terrorists networks to advanced nation states. Defending against these threats to our security, prosperity, and personal privacy requires networks that are secure, trustworthy, and resilient. Our digital infrastructure, therefore is a strategic national asset, and protecting it—while safeguarding privacy and civil liberties—is a national security priority.[49]

Based upon the strategic importance of cyberspace to all developed states, the domain has emerged as a critical vulnerability to those that rely upon it to run their infrastructure, power generation, economies, and communications.

Due to cyberspace's wide-scale vulnerability, coupled with its low cost entry barriers and permissive operating environment, the domain is rapidly changing the

character of war. As an enabling force, cyber warfare can prepare the battlefield for conventional forces by aiding intelligence gathering, paralyzing an adversary's command and control systems; disrupting enemy early warning capability, and wreaking havoc within enemy logistical systems. As a strategic force, cyber warriors can attack enemy centers of gravity through seams and vulnerabilities.

Many opponents of the cyber warfare's decisiveness contend that the types of capabilities outlined above provide the extent of this domain's usefulness. Without the ability to create casualties or occupy land, cyber warfare's strategic effectiveness is speculative at best and lacks any true concrete examples of coerciveness.[50] Critics purport that an agile enemy will react quickly to limit the effects of a cyber first strike, close vulnerabilities, and repair damages without long-term persistent damage. Furthermore, they argue that CNA can only be used against actors with a high degree of connectedness and vulnerable cyber targets.[51]

While these critics raise many interesting points, they overlook the theoretical plausibility of future CNA capability as well as developed but untested or classified capability. Often critics of cyber warfare discount its ability to inflict persistent damage comparable to conventional weapons, yet the effects of both are often negated by a skilled adversary's repair capacity. Both conventional and CNA provide an effect at a certain point and time, but neither are permanent. While CNA will not destroy an enemy force, it can disrupt their effectiveness by targeting command and control networks, injecting false data to impede decision making, or degrading networked targeting solutions to point which exceeds collateral damage tolerances. Ultimately, a lack of past

examples does not detract from future application and resultant strategic decisiveness of cyber warfare.

Assumptions

The conduct of strategic cyber warfare requires a number of assumptions for its success. These assumptions do not correlate to the ease of attaining the prescribed conditions. The assumptions listed below are not an exclusive list but characterize some of the necessary conditions for a successful strategic cyber warfare strategy:

- Intelligence is available to determine vulnerable adversary systems
- Sufficient knowledge exists of system vulnerabilities to inject malware to achieve intended results
- Expertise is available to devise appropriate CNA
- Time is available to generate effects or have attack promulgate to intended system
- Possess the ability to attack redundant systems
- Possess the ability to overcome deception, detection, firewalls and air-gapped networks
- Political support and will is sufficient for cyber warfare operations and continue despite adversary reprisals

Parallel Strategic Application

Cyber warfare theories and application are not too distant from other domains of warfare. For example, early airpower theorist Giulio Douhet saw the utility in a style of maneuver warfare which bypassed an adversary's fielded forces and directly attacked its centers of gravity. While Douhet's theories are not entirely analogous, his advocating

of the offensive use of aerial forces to target city population centers, industrial and economic means, and transportation arteries to break the will of the people and achieve decisive strategic results has many similarities to the strategic employment of cyber warfare.[52] Douhet's assertions that the offensive bomber could break the will of the people were unrealized in World War II for a number of reasons. Most important, air power was unable to deliver persistent and precision strategic effects to the enemy's centers of gravity. Furthermore, in the post World War II era, policy restrictions inhibited the full potential of air power. Whereas Douhet failed to anticipate limits on warfare, Clausewitz recognized its need. "Policy, then will permeate all military operations, and, in so far as their violent nature will admit, it will have a continuous influence on them."[53]

When survival interests are at stake, history has demonstrated that states and their populous are resilient to conventional attack and their will is not easily broken. For example, the bombing of London actually increased the resolve of the British populous. In this example, survival interests were at stake. Should a conflict ensue that falls short of survival interests, could a state be influenced to change its course of action and bend to another's will entirely by the effects of CNA? A surprise cyber attack of an adversary's military-related civilian targets in parallel with a cyber attack upon its fielded forces can provide crippling short-term effects.[54]

> In short, the difficulty of defending against a surprise attack launched against military-affiliated logistical networks or a 'decapitation' attack launched against command and control systems – which could potentially cripple the target state's conventional military forces and dramatically increase the effectiveness of any subsequent use of conventional force – suggests that cyber warfare capabilities may significantly favor the offensive advantage.[55]

This statement by Princeton's Department of Politics Doctoral Candidate, Adam Liff is insightful on two accounts. First, it postulates the effectiveness of CNA on

adversary systems, but more importantly the statement supports the value of the cyber domain as an offensive weapon. It is this offensive capability which enables cyber warfare to be employed with decisive results.

Although cyber warfare has two key components (CNA and CND), the offensive character of CNA enables its decisiveness if used in conjunction with a well-crafted strategy. As with all forms of warfare, the application of cyber power is an art which requires an in-depth operational design and planning process. Creating strategic level effects begins with a thorough understanding of the operational environment and the problem. Included in the operational environment is a study of adversary culture, demographics, infrastructure, decision-making processes, and operational capability.[56] Gaining this familiarity is key to identifying enemy centers of gravity and critical vulnerabilities and cannot be shortcut by applying a preconceived menu of cyber options.

Additionally, a thorough analysis is crucial to the proper application of cyber power. Not all adversaries are vulnerable to a strategic cyber attack. Those adversaries with a low degree of interconnectedness and less developed economies will require a traditional multispectrum warfare approach. However, as time progresses, more and more states will develop their cyber infrastructures while simultaneously increasing their vulnerabilities to CNA.

Regardless of a nation’s dependence on its cyber infrastructure, a cyber war will only be decisive when strategic objectives are limited. When survival interests are threatened, states are not likely to submit while they have the means to resist. However,

a limited war against a vulnerable enemy presents an opportunity to leverage the strategic value of cyber warfare.

In a strategic cyber war, the principles of surprise, the offensive, mass, and maneuver are critical because every adversary will attempt to counter an attack.[57] By overwhelming an adversary through persistent and massed effects on critical vulnerabilities the likelihood of capitulation increases. Still, this window of opportunity is finite, as a population's resolve potentially increases with time as they learn to endure the "hurt" inflicted by CNA. This scenario is analogous to an extended bombing campaign. As a result, a rapid cyber war has a greater likelihood of breaking the will of an enemy and delivering decisive results.

As stated above, the opportunity for a successful cyber war increases when strategic endstates are limited and territorial integrity or survival interests are not threatened. For instance, following Iraq's invasion of Kuwait, the U.S. led coalition's strategic end state did not include the destruction of Iraq or a regime change. Instead, the coalition sought Iraq's unconditional withdrawal from Kuwait.[58] In similar scenarios cyber warfare could provide the necessary strategic effects without the expense and time needed for a six-month build-up of friendly conventional forces. A rapid cyber offensive focused on enemy centers of gravity can shape an adversary's will if the strategic endstate is limited. While cyber warfare shares some similarities to strategic air power, the former can manifest widespread paralysis within the government, military, industry, and civilian sectors without violating the principles of LOAC. Once this level of hurt is no longer acceptable, a populous will leverage its government to sue for peace.

To date the strategic effectiveness of cyber warfare is untested. Furthermore, many assumptions must be made in order to theorize the decisiveness of cyber warfare. However, theorists past and present concede the possibility of victory without bloodshed. Clausewitz “postulates that, to bend the enemy to your will, you must ‘either make him literally defenceless [sic] or at least put him [in] a position that makes this danger probable.’”[59] The use of CNA on centers of gravity in conjunction with the threat of a conventional attack have the effect of increasing the danger to a point where the people and the government conclude they are defenseless to an attack.

Conclusion

The emergence of the cyber domain has had a profound influence on future war planning. Cyber capability now permeates nearly every tool used to wage or command and control war. Conventional weapons, communication, and information systems depend upon assured, reliable, and resilient network access. These inherent vulnerabilities coupled those within the civilian sector have precipitated the genesis of cyber warfare.

The use of CNA has steadily increased over the past decade. Lapses in cyber security resulted in the pilfering of hundreds of billions of dollars worth of intellectual property, military and industry secrets, and banking securities. Cyber warfare has evolved so quickly that international norms and laws have failed to keep pace with the effects it can project. As a result, ambiguous treaties and conventions meant to constrain the conventional use of armed force do not conveniently translate to the cyber domain, nor has there been a substantial political effort or desire to adopt these rules to the cyber domain.

Despite cyber warfare's relative infancy, its speed, range, cost, accessibility, and range of effects undoubtedly have changed the character of war. While all of these characteristics truly redefined this type of warfare's style it falls short of changing its enduring nature. At its core, cyber war is still a rational instrument of policy that is subject to uncertainty and has the potential to attain effects with a high degree of violence.

Most important to the nucleus of this paper is whether or not cyber warfare can be decisive in a limited war. There is little contention that cyber warfare is an outstanding force multiplier and enabler, but with current technology, cyber can also attack an adversary's centers of gravity and create strategic effects. Through rapid offensive action, cyber warfare has not only changed the character of war, but can also create the necessary effects to achieve strategic decisiveness.

Endnotes

[1] U.S Department of Defense, Department of Defense Strategy for Operating in Cyberspace (Washington DC: U.S. Department of Defense, July 2011), 3.

[2] An actor is defined as an entity (state, institution, group, or individual) that has the ability to influence its environment.

[3] Barack H. Obama, *Cyberspace Policy Review: Assuring Trusted and Resilient Information and Communication Infrastructure* (Washington, DC: The White House), 2.

[4] Kristen M. Finklea and Catherine A. Theohary, *Cyber crime: Conceptual Issues for Congress and U.S. Law Enforcement* (Washington, DC: U.S. Library of Congress, Congressional Research Service, July 20, 2012), 7, http://www.fas.org/sgp/crs/misc/R42547.pdf (accessed February 2, 2013).

[5] U.S. Secretary of Defense, Leon Panetta's speech to the Business Executives for National Security in New York City on October 11, 2012 described recent security issues targeting cyber infrastructure. Distributed Denial of Service attacks against U.S. banking interests disrupted client service, while another malware virus created widespread damage in Saudi Arabia's state oil company Aramco. "Shamoon included a routine called a 'wiper', coded to self-execute. This routine replaced crucial systems files with an image of a burning U.S. flag. But it also put additional garbage data that overwrote all the real data on the machine. More than 30,000 computers that it infected were rendered useless and had to be replaced. It virtually

destroyed 30,000 computers." A similar attack occurred shortly after in Qatar. Panetta cautioned the audience that attacks such as this coupled key simultaneous attacks on critical infrastructure could potential result in a "cyber Pearl Harbor." Leon Panetta, "Secretary Leon Panetta's Speech about Cybersecurity," October 11, 2012, http://www.cfr.org/cybersecurity/secretary-leon-panettas-speech-cybersecurity/p29262 (accessed February 3, 2013).

[6] Jayson M. Spade, *Information as Power: China's Cyber Power and America' National Security*, ed. Jeffrey L. Caton (Carlisle Barracks: United States Army War College, 2012), 9.

[7] Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *The Journal of Strategic Studies* 35, no. 3 (June 2012): 404, in ProQuest (accessed October 30, 2012).

[8] Spade, *Information as Power*, 9.

[9] Stuxnet was conceived during the George W. Bush administration and continued by the Obama administration. The malware was ultimately discovered in 2010. Norman Asa, "Cyberattacks on Iran – Stuxnet and Flame." *New York Times*. August 9, 2012, http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html (accessed February 6, 2013).

[10] Kenneth Lieberthal and Peter W. Singer, *Cybersecurity and U.S.-China Relations* (Washington DC: Brookings Institution, 2012), 10, http://www.brookings.edu/~/media/research/files/papers/2012/2/23%20cybersecurity%20china%20us%20singer%20lieberthal/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf (accessed on December 16, 2012); Spade, *Information as Power*, 9.

[11] Shmuel Even and David Siman-Tov, *Cyber Warfare: Concepts and Strategic Trends,* Memorandum No. 117 (Tel Aviv: Institute for National Security Studies, 2012), 54.

[12] CJCSI 3121.01B, Standing Rules of Engagement/Standing Rules for the Use of Force for U.S. Forces (13 June 2005). 88, https://www.jagcnet.**army**.mil (accessed on December 12, 2012).

[13] Colin S. Gray, *The Strategy Bridge: Theory for Practice* (Oxford: Oxford University Press, 2010), 7-8.

[14] U.S. Air Force Chief of Staff, *Basic Doctrine, Organization, and Command*, Air Force Doctrine Document 1 (Washington, DC: U.S. Air Force Chief of Staff, October 14, 2011), 25.

[15] Carl von Clausewitz, *On War,* ed. and trans. Michael Howard and Peter Paret. (Princeton, NJ: Princeton University Press, 1976), 75.

[16] Ibid., 605.

[17] Leonard J. Fullenkamp, "Carl von Clausewitz and Contemporary Views about Strategy and War," lecture, U.S. Army War College, Carlisle Barracks, PA, September 10, 2012, citied with permission of Dr. Fullenkamp; Clausewitz, On War, 89.

[18] Clausewitz, *On War*, 75.

[19] Ibid., 91.

[20] Ibid., 92.

[21] Ibid., 606.

[22] Ibid., 85; Colin S. Gray, *War, Peace and International Relations* (New York: Routledge, 2007), 227.

[23] Colin S. Gray, *Another Bloody Century: Future Warfare* (London: Weidenfeld & Nicolson, 2005), 24.

[24] Ibid., 324.

[25] Clausewitz, *On War*, 85.

[26] Even and Siman, *Cyber Warfare: Concepts and Strategic Trends*, 35.

[27] David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (New York: MPG Books, 2004), 31.

[28] Lonsdale, *The Nature of War*, 213.

[29] Clausewitz, *On War*, 90.

[30] Ibid.

[31] Gray, *Another Bloody Century*, 201.

[32] Liff, "Cyberwar: A New 'Absolute Weapon'," 403-404.

[33] About.com, "US Military," http://usmilitary.about.com/cs/wars/a/loac.htm (accessed January 8, 2013).

[34] Ibid.

[35] Jeffrey Carr, *Inside Cyber Warfare* (Cambridge: O'Reilly, 2010), 39.

[36] The United Nations Homepage, "The Charter of the United Nations and Statute of the International Court of Justice," June 26, 1945, http://www.un.org/en/documents/charter/index.shtml (accessed December 12, 2012).

[37] UN Charter, art 39.

[38] UN Charter, art 51.

[39] Matthew J. Sklerov, "Responding to International Cyber Attacks as Acts of War," in *Inside Cyber Warfare*, ed. Jeffrey Carr (Cambridge: O'Reilly, 2010), 50.

[40] Ibid., 59.

[41] Ibid.

[42] Ibid.

[43] Schreir, *On Cyberwarfare,* 69.

[44] While international law lacks specificity regarding cyber warfare, there have been strides in addressing cyber crime. Many members of the international community worked to address what constitutes a cyber crime at the Council of Europe Convention on Cyber crime held in Budapest in 2001. This group made initial progress on standardizing legal domestic frameworks and intergovernmental cooperation procedures for combating cyber crime. This convention makes an important first step toward a cooperative effort by the international community in recognizing and taking positive steps to address the malicious use of the cyber domain. Finklea and Theohary, *Cybercrime: Conceptual Issues*, 15.

[45] Even and Siman, *Cyber Warfare: Concepts and Strategic Trends*, 14-18.

[46] Matthew Crosston, "Virtual Patriots and a New American Cyber Strategy: Changing the Zero-Sum Game," *Strategic Studies Quarterly* 6, no. 4 (Winter 2012): 102.

[47] Schreir, *On Cyberwarfare,* 7.

[48] Ibid., 7.

[49] Barack H. Obama, *National Security Strategy* (Washington, DC: The White House, May 2010), 20; Michael G. Mullen, *The National Military Strategy of the United States of America 2011: Redefining America's Military Leadership* (Washington, DC: The Pentagon, February 2011), 27.

[50] Martin C. Libicki, *Cyberdeterrence and Cyberwar*, (Arlington: RAND, 2009), 122, 123, 137, http://www.rand.org/publications/permissions.html (accessed November 4, 2012).

[51] Ibid., 120.

[52] Giulio Douhet, *The Command of the Air*, trans. Dino Ferrari (New York: Coward-McCann, 1942), 20.

[53] Clausewitz, *On War*, 87.

[54] Libicki, *Cyberdeterrence and Cyberwar*, 137, 139, 142.

[55] Liff, "Cyberwar: A New 'Absolute Weapon'," 415.

[56] Michael G. Mullen, *Joint Publication (JP) 5-0, Joint Operational Planning* (Washington, DC: The Pentagon, August 11, 2011), III-9.

[57] U.S. Air Force Chief of Staff, *Basic Doctrine AFDD 1, 30.*

[58] George H. W. Bush, National Security Directive 54 (Washington, DC: The White House, January 15, 1991), 2, http://www.fas.org/irp/offdocs/nsd/nsd54.pdf (accessed January 29, 2013).

[59] Lonsdale, *The Nature of War*, 31.